# Level Set Methods for Computing Reachable Sets of Hybrid Systems with Differential Algebraic Equation Dynamics

AUTHOR(S):

Mitchell, Ian M.; Susuki, Yoshihiko

# Level Set Methods for Computing Reachable Sets of Hybrid Systems with Differential Algebraic Equation Dynamics

Ian M. Mitchell[1] and Yoshihiko Susuki[2]

[1] Department of Computer Science, University of British Columbia,
2366 Main Mall, Vancouver, BC, Canada V6T 1Z4
mitchell@cs.ubc.ca
http://www.cs.ubc.ca/∼mitchell
[2] Department of Electrical Engineering, Kyoto University,
Katsura, Nishikyo, Kyoto, Japan 615–8510
susuki@dove.kuee.kyoto-u.ac.jp
http://www-lab23.kuee.kyoto-u.ac.jp/susuki

**Abstract.** In previous work we demonstrated that reachability algorithms using level set methods and based on the Hamilton-Jacobi PDE can be adapted to systems whose dynamics are described by differential algebraic equations. Here we extend those results to hybrid systems. The only significant addition required is a mechanism for handling the state reset that occurs during discrete jumps between modes. We demonstrate the technique on a nonlinear power system voltage safety problem.

## 1 Introduction

The reachable set or tube is an effective tool for verification, but it can rarely be determined exactly for hybrid or continuous systems. Many approximate reachability algorithms have been proposed, and we refer to [1] and the citations within for further discussion of such algorithms. A central assumption of virtually all algorithms has been that the continuous dynamics of the system are modeled by ordinary differential equations (ODEs). The differential algebraic equation (DAE) is a generalization of the ODE, and in previous work [2] we described how to adapt reachability algorithms based on level set methods and the Hamilton-Jacobi (HJ) partial differential equation (PDE) to approximate the backwards reachable tube for continuous systems modeled by DAEs. Here we demonstrate how to extend the algorithm to hybrid systems in which DAEs drive the continuous dynamics through a hybrid version of the nonlinear power system voltage safety scenario. We do not have room in this brief paper to provide all of the details, but code containing those details and recreating the results below can be found at [3].

Given a system state space $\mathbb{S}$ and a set of known unsafe states $T \subset \mathbb{S}$, we seek to approximate the backwards reachable tube

$$B(T,[0,t]) \triangleq \{x_0 \in \mathbb{S} \mid \exists \hat{x} \in T, \exists s \in [0,t], x(s) = \hat{x}\},$$

where $x(\cdot)$ is a trajectory of the system starting at $x(0) = x_0$. For systems whose continuous trajectories are specified by ODEs, we described in [4] how the reachable tube for some fixed $t$ can be implicitly defined as $B(T, [0, t]) = \{x \in \mathbb{S} \mid \phi(x) \leq 0\}$, where $\phi : \mathbb{S} \to \mathbb{R}$ is the viscosity solution of an HJ PDE (if $t$ may vary, $\phi$ will depend on $t$). The method is extended to continuous systems specified by index one DAEs in [2].

We will not address here the theoretical questions that arise when substituting DAEs for ODEs in a hybrid automata (HA) model, and therefore avoid a formal HA definition. The primary computational challenge of extending the procedure from [2] to a hybrid setting is the implicitly defined jump that occurs in the continuous state when a discrete mode switch causes a change in the governing DAE. We describe below how to convert this implicit jump into an explicit reset map, and then how to map the implicit surface representation of the reach tube $\phi$ through this reset.

## 2 Mapping the Reachable Tube across Mode Jumps

In a DAE model the standard ODE $\dot{x}(s) = f(x(s))$ is replaced by a coupled set of differential and algebraic equations. We focus on index one DAEs which can be written in semi-explicit form as

$$\dot{y}(s) = f_{\mathbb{D}}(y(s), z(s); p) \tag{1}$$
$$0 = g(y(s), z(s); p) \tag{2}$$

where the state $x = (y, z)$ is divided into differential variables $y$ and algebraic variables $z$, and $p$ are some known parameters. In a hybrid system with modes denoted by variable $q$, the parameters will depend on the mode $p = p(q)$. Under appropriate conditions, such DAEs can be understood as the ODE (1) evolving on the constraint manifold $C(p) = \{(y, z) \mid g(y, z; p) = 0\}$. We described two procedures for approximating the reachable tube of a continuous system modeled by (1)–(2) in [2]. In the hybrid system extension, either procedure may be used for the continuous evolution of the reachable tube.

Consider now the effect of a discrete jump in the HA from a mode $q^-$ with parameters $p^- = p(q^-)$ to a mode $q^+$ with parameters $p^+ = p(q^+)$. As we are working with backwards reachability, we assume that an implicit representation of the backwards reachable tube is available for mode $q^+$ in the form $\phi^+(x)$, and we wish to find a representation for mode $q^-$ in the form $\phi^-(x)$ (after which continuous evolution in mode $q^-$ will begin). We seek a reset mapping $x^+ = \rho(x^-, p^-, p^+)$ so that we can construct $\phi^-(x) = \phi^+(\rho(x, p^-, p^+))$.

In a standard HA this reset mapping $\rho$ is given explicitly [4], but in the DAE model it is implicit. To determine $\rho$ we assume that the constraint (2) arises in the limit $\epsilon \to 0$ from some "fast" dynamics given by the ODE $\epsilon \dot{z} = g(y, z; p)$. When a discrete mode switch causes a change in parameters such that $g(y^-, z^-; p^+) \neq 0$, we fix $y^+ = y^-$ (since $y$ governed by (1) cannot react fast enough) and solve the ODE $\dot{z} = g(y^+, z; p^+)$ with initial condition $z(0) = z^-$ in auxiliary "fast" time to a fixpoint $\lim_{t\to\infty} z(t) = z^+$.

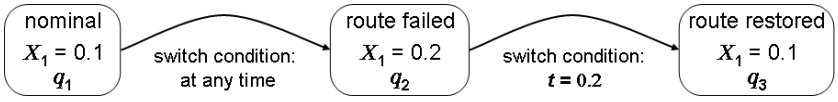



**Fig. 1.** Hybrid automaton for the example.

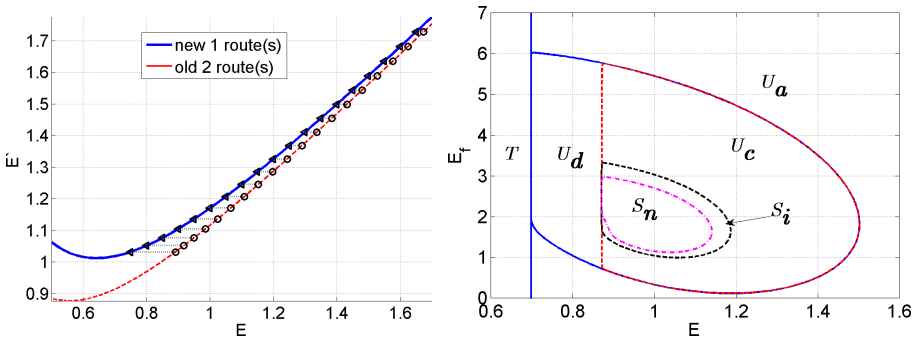
## 3 Single Machine-Load Bus Example

We now demonstrate our reset mapping procedure on a concrete example. For the continuous dynamics, we use a three dimensional DAE model of a single machine-load bus from [5]. For lack of space we are forced to omit all of the details of the continuous model; the discussion that follows may not make much sense without first reading those details in [2]. All three state variables $(E', E_f, E)$ are voltages. The state variables $E'$ and $E_f$ appear in the differential component of the DAE (they correspond to differential variable $y$), while the algebraic constraint relates $E$ and $E'$ (so $E$ corresponds to algebraic variable $z$) in a manner dependent on a parameter $p = X_1$. Note that the prime is not a derivative—$E'$ is a separate variable from $E$. The discrete component of the HA for the system is shown in figure 1; it and the safety analysis problem are adapted from [6], where interested readers can also find further discussion of related work on power system models.

In words, the HA in figure 1 describes a scenario in which the system starts in its nominal operating mode $q_1$ with two transmission routes and parameter $X_1 = 0.1$. An uncontrollable event may cause one route to fail at any time, and the system jumps into a single route mode $q_2$ with $X_1 = 0.2$. The failure is detected after a brief period (12 cycles at 60 Hertz is 0.2 seconds) and relays switch in a backup route to restore the system to its nominal parameter $X_1 = 0.1$ in mode $q_3$. The unsafe behaviour of the system is that the load bus voltage $E$ may drop below a defined minimum value $E_c = 0.7$. The failure may occur due to continuous oscillations in the voltages and/or due to discrete voltage jumps when the number of transmission routes change.

Figure 2(a) shows samples of the reset mapping $\rho$ for the $q_1$ to $q_2$ switch, as well as the constraint surfaces for the two values of $X_1$. The plot is in the $E$ vs $E'$ plane because the constraint does not depend on $E_f$. When working with level set methods, $\phi$ is stored on a discrete grid. Consequently, we only need to determine $\rho(x, p^-, p^+)$ where $x$ is a node of the grid—a finite number of samples. We then use interpolation on $\phi^+$ to construct a value for $\phi^-$, since $\rho(x, p^-, p^+)$ will not generally be a node in the grid even if $x$ is.

In [2] we approximated the set of states leading to continuous failure in the nominal operating mode $q_1$ without any switches (although we used a different value of parameter $Q_0$ in those calculations). Two algorithms were proposed: one that works on the constraint manifold and one that works in the full dimensional state space. We show only the former here, although the reset mapping procedure is easily extended to the latter. For our coordinate system on the constraint manifold we choose $E$ and $E_f$, so the reachable tubes shown are essentially projections of the full dimensional reachable tubes onto these two variables. Figure 2(b) shows the results of the reachability analysis on the manifold.




(a) The constraint surfaces $C(X_1)$ and samples of the reset mapping $\rho$. The reset mapping goes from states labeled by circles to states labeled by triangles.

(b) The reachability results for the example with parameter $Q_0 = 0.25P_m$ (if $Q_0 = 0.5P_m$ from [2] were used, there would be no safe states).

**Fig. 2.** Results for the example. Note that the vertical axes are different variables in the two plots. The sets labeled in the right subplot are: known unsafe target set $T$, states unsafe in the nominal mode with no discrete switching $U_a$, states that become unsafe during discrete switches $U_d$, states which become unsafe due to a combination of discrete and continuous evolution $U_c \cup S_i$, and safe states $S_n$ for mode $q_1$ of the HA from figure 1. If there was no 12 cycle delay in detecting the route failure, the safe states would be $S_n \cup S_i$. If there was never a route failure (the situation examined in [2]), the safe states would be $S_n \cup S_i \cup U_c \cup U_d$.

## References

1. I. M. Mitchell, "Comparing forward and backward reachability as tools for safety analysis," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds. Springer Verlag, 2007, no. 4416, pp. 428–443.
2. E. A. Cross and I. M. Mitchell, "Level set methods for computing reachable sets of systems with differential algebraic equation dynamics," submitted September 2007 to American Control Conference, 7 pages. [Online]. Available: http://www.cs.ubc.ca/~mitchell/Papers/submittedReachDAE.pdf
3. [Online]. Available: http://www.cs.ubc.ca/~mitchell/ToolboxLS
4. C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986–1001, July 2003.
5. V. Venkatasubramanian, H. Schättler, and J. Zaborszky, "Voltage dynamics: Study of a generator with voltage control, transmission, and matched MW load," *IEEE Transactions on Automatic Control*, vol. 37, no. 11, pp. 1717–1733, November 1992.
6. Y. Susuki and T. Hikihara, "Predicting voltage instability of power system via hybrid system reachability analysis," in *Proceedings of the American Control Conference*, New York, NY, 2007, pp. 4166–4171.